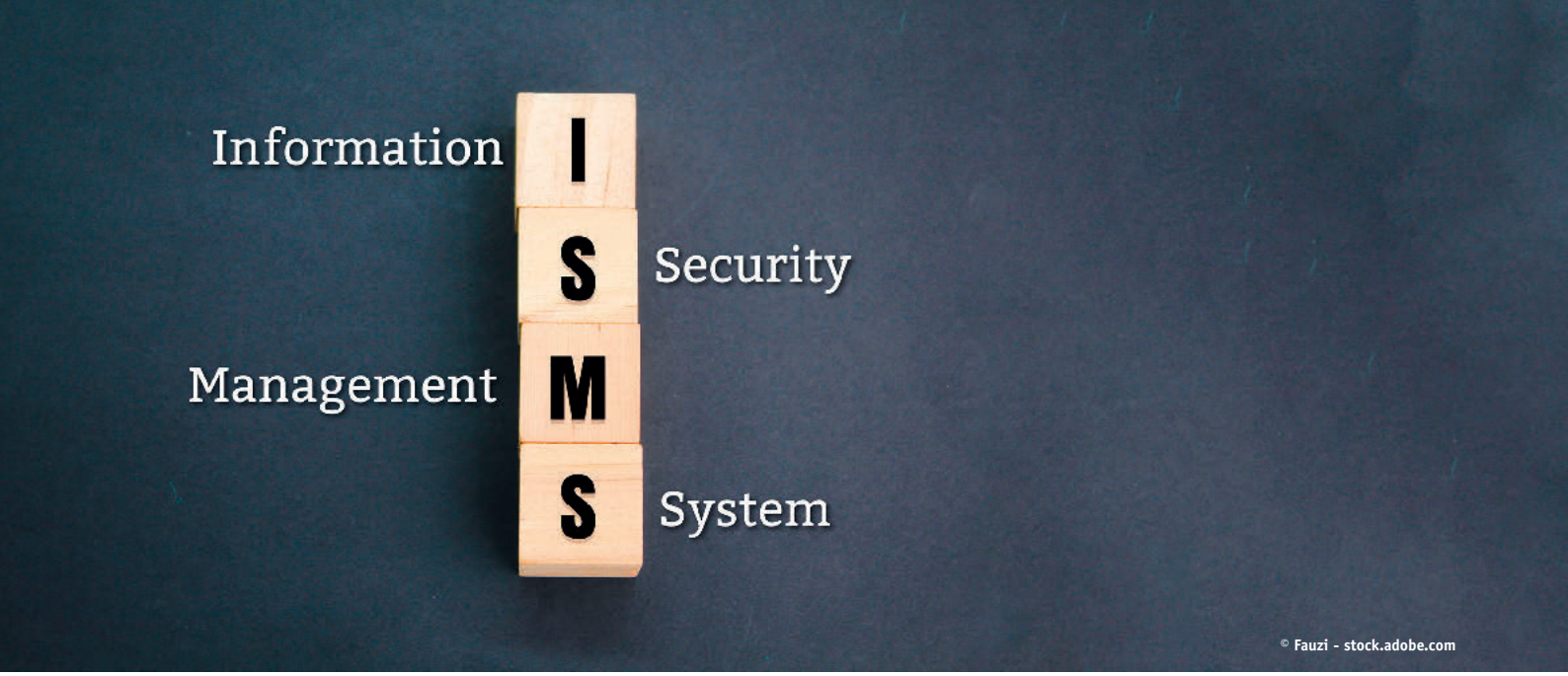

Das Informationssicherheitsmanagementsystem (ISMS) im Krankenhaus

Best Practices für die Implementierung

Von Alexander Miller, Peter Maximiliam Conrad und Benjamin Rebholz

Die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) ist für jedes Krankenhaus empfehlenswert. Diese Aufgabe stellt jedoch eine komplexe Herausforderung dar, weshalb die Umsetzung in vielen Krankenhäusern oft vernachlässigt oder nur konzeptionell angegangen wird. Für eine erfolgreiche Etablierung sind Veränderungen auf allen Ebenen des Krankenhauses erforderlich. Entscheidend sind dabei die Unterstützung und das Verständnis der Führungsebene, der effiziente Einsatz von Ressourcen sowie die Einbindung und Mitnahme der gesamten Krankenhausbelegschaft.

Keywords: *Digitalisierung, Innovation, IT*

In den vergangenen Jahren häufen sich in Deutschland Schlagzeilen wie: „Cyberangriff auf Krankenhaus: Dutzende Operationen verschoben." Angriffe auf kritische Infrastrukturen (KRITIS) haben zugenommen, was sich in der steigenden Anzahl gemeldeter Cybervorfälle widerspiegelt. Bis November 2024 wurden innerhalb der KRITIS 726 Vorfälle gemeldet, was einem Anstieg von 48 Prozent im Vergleich zum Vorjahr entspricht. Fast 20 Prozent dieser Vorfälle betreffen Einrichtungen des Gesundheitswesens, insbesondere Krankenhäuser. Cybervorfälle in Krankenhäusern verursachen nicht nur wirtschaftliche Schäden, sondern gefährden insbesondere die medizinische Versorgung der Bevölkerung. Krankenhäuser müssen beispielsweise die Notaufnahme abmelden oder Intensivpatienten in andere Krankenhäuser verlegen. Im schlimmsten Fall sind Menschleben bedroht. Zudem sind die im Krankenhaus erhobenen und genutzten sensiblen Gesundheitsdaten besonders schützenswert, da ein Verlust oder Missbrauch dieser Daten schwerwiegende Folgen für die Patienten und die Reputation des Krankenhauses haben kann. Um diesen Bedrohungen entgegenzuwirken, ist die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) in Krankenhäusern von entscheidender Bedeutung. Erfahrungsgemäß wird die Umsetzung eines ISMS in vielen Krankenhäusern jedoch oft vernachlässigt oder bleibt lediglich auf konzeptioneller Ebene, was auf unzureichendes Bewusstsein für die Bedeutung der Informationssicherheit, mangelnde Priorisierung und begrenzte Ressourcen zurückzuführen ist.

Ein ISMS stellt einen systematischen Ansatz dar, um die Informationssicherheit (Abb. 1) und den Datenschutz in einer Organisation zu gewährleisten. Es umfasst die Aufstellung von Verfahren und Regeln, die dazu dienen, die Informationssicherheit dauerhaft zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Dabei schützt es Informationen vor Gefahren wie Cyberangriffen, internen Bedrohungen, Programmier- und Systemfehlern sowie physischen Risiken.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem IT-Grundschutz ein Konzept für die Umsetzung eines ISMS entwickelt. Der IT-Grundschutz bietet mit seinen Standards 200–1, 200–2 und 200–3 sowie

den IT-Grundschutzkatalogen Hilfestellungen bei der Einführung und Aufrechterhaltung eines ISMS und ist an die internationale Norm ISO/IEC 27001 angepasst.

Nach dem BSI-Standard 200–1 gehören zu einem ISMS folgende grundlegenden Komponenten:

- Managementprinzipien: Leitlinien, Ziele und Strategien, die von der Leitungsebene festgelegt werden, um die Informationssicherheit zu steuern und zu lenken.
- Ressourcen: Bereitstellung und Verwaltung der notwendigen Mittel, einschließlich finanzieller, technischer und personeller Ressourcen, um die Informationssicherheit zu gewährleisten.
- Mitarbeiter: Einbindung und Schulung der Mitarbeiter, um sicherzustellen, dass diese die Sicherheitsrichtlinien verstehen und umsetzen können.
- Sicherheitsprozesse: Planung, Implementierung, Überwachung und kontinuierliche Verbesserung der Sicherheitsmaßnahmen und -verfahren. Dazu gehören die ISMS-Leitlinie, das Sicherheitskonzept und die Sicherheitsorganisation.

Der Aufbau und Betrieb eines ISMS folgt dem Plan-Do-Check-Act-Zyklus (PDCA-Zyklus, Abb. 2):

1. **Plan:** Erstellung einer ISMS-Leitlinie und grundlegender Dokumente. Dabei müssen entscheidende Fragen geklärt werden, beispielsweise welche Ziele mit dem ISMS verfolgt werden.
2. **Do:** Identifikation und Klassifikation von schützenswerten Assets sowie der Aufbau der ISMS-Organisation und Risikomanagement-Strukturen.
3. **Check:** Entwicklung und Implementierung von Kontrollmechanismen, Dokumentation sowie Umsetzung von Prozessen.
4. **Act:** Anpassung und Erweiterung des ISMS auf Basis gesammelter Erfahrungen.

Unterstützung der Führungsebene als Schlüsselfaktor

Eine erfolgreiche Implementierung eines ISMS erfordert die uneingeschränkte Unterstützung der Führungsebene, die in der Praxis häufig aufgrund anderer Prioritäten oft nicht gewährleistet ist. Daher ist es essenziell, zunächst das Bewusstsein für die Bedeutung der Informationssicherheit und die damit verbundene Haftung zu schärfen. Die Führungsebene muss verstehen, dass Informationssicherheit eine Führungsaufgabe ist und sie bei unzureichender Implementierung haftbar gemacht werden kann. Deshalb sollte bei der Implementierung eines ISMS regelmäßig an die Führungsebene über Fortschritte und Erfolge berichtet werden. Ebenso wichtig ist es, dass die Führungsebene die Bedeutung des ISMS kontinuierlich an alle Beteiligten kommuniziert, einschließlich des aktuellen IST-Zustands des ISMS.

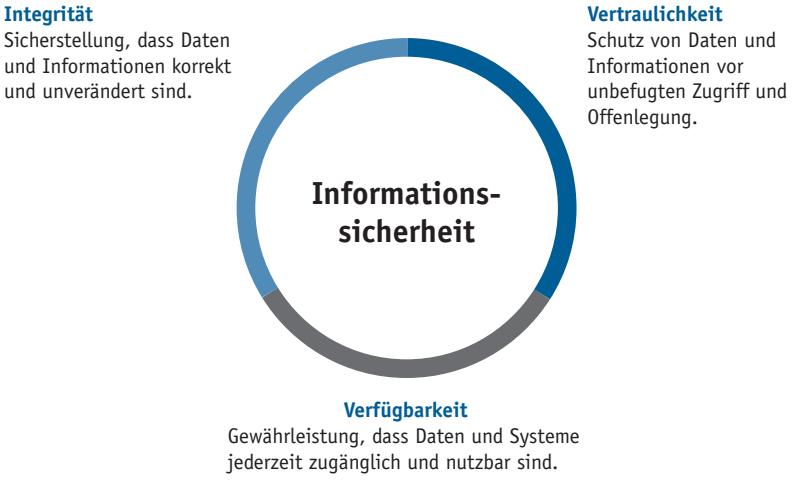

Abb. 1: Schutzziele der Informationssicherheit, die mithilfe der Etablierung eines ISMS im Krankenhaus gewährleistet werden sollen.

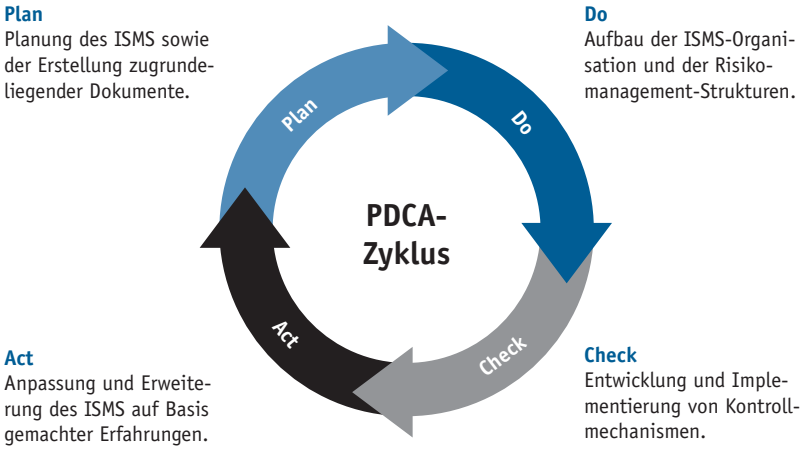

Abb. 2: In Anlehnung an BSI-Standard 200–1, Seite 18 Abbildung 5. Ablauf der Etablierung eines ISMS anhand des PDCA-Zyklus.

Etablierung neuer Rollen und Gewährleistung des Wissenstransfer

Ungeachtet der zur Verfügung stehenden Ressourcen sollte in jedem Krankenhaus ein Informationssicherheitsbeauftragter (ISB) existieren. Häufig mangelt es jedoch an der Personalstärke oder an den Qualifikationen. Das BSI stellt dahingehend eine Liste mit zertifizierten Organisationen zur Verfügung, die Lehrgänge zu den Themen Informationssicherheit und ISMS anbieten. Zudem existiert die Möglichkeit, externe Personen als ISB zu beauftragen. Dabei bleibt die Gesamtverantwortung für die Informationssicherheit weiterhin bei der Führungsebene des Krankenhauses bestehen.

Bei der Umsetzung eines ISMS ist es zudem erforderlich, neben dem ISB zusätzliche Rollen zu etablieren und bestehende Verantwortlichkeiten neu zu definieren. Es ist wichtig, diese Rollen gemeinsam mit den Beteiligten zu besetzen, um deren Akzeptanz und Engagement sicherzustellen. Personen, die diese Rollen übernehmen, sollten über die notwendigen Befugnisse und Freiräume verfügen sowie die erforderlichen Qualifikationen und Softskills mitbringen. Gleichzeitig sollten vorhandene Rollen und Prozesse nach Möglichkeit optimal integriert werden, da dies die Etablierung eines ISMS erheblich erleichtert und das bestehende Wissen im Krankenhaus genutzt werden kann.

In der Praxis hat sich jedoch gezeigt, dass etablierte Prozesse, zugewiesene Rollen und das Bewusstsein für Gefahren häufig nur unzureichend ausgeprägt sind. Regelmäßige Übungen finden nicht statt und die Weitergabe von

Beispiel Checkliste: Sofortmaßnahmen bei einem Ransomware-Angriff

Die Checkliste richtet sich an Mitarbeiter, deren System von einem Ransomware-Angriff betroffen ist, und unterstützt sie bis zur Übergabe an die IT-Abteilung bzw. den ISB.

#	Aktivität	Zuständig	Erledigt
1.	Foto des Desktops erstellen, um Beweise zu sichern.	Meldende Person	
2.	Verbindung zum Netzwerkt trennen bzw. Netzwerkkabel / LAN-Kabel aus dem betroffenen System (z. B. Computer) ziehen.	Meldende Person	
3.	Meldung an IT-Abteilung oder ISB durchführen Telefonnummer IT-Abteilung: <einfügen> Telefonnummer ISB: <einfügen>	Meldende Person	
4.	Anweisungen des ISB oder der IT-Abteilung folgen.	Meldende Person	
5.	Übergabe der gesicherten Beweise an die IT-Abteilung oder den ISB.	Meldende Person	

Ab diesem Schritt übernimmt die IT-Abteilung bzw. der ISB die Kontrolle über den Vorfall. Sie sollten weiterhin für Rückfragen und zur Lösung des Vorfalls zur Verfügung stehen. Es ist ratsam, ein Gedächtnisprotokoll anzulegen, damit keine entscheidenden Informationen verloren gehen.

Tab.: Beispiel einer Checkliste für Mitarbeiter im Falle eines Ransomware-Angriffs.

Informationen erfolgt unvollständig. Es ist daher ratsam, vor Beginn der Etablierung eines ISMS die bestehenden Rollen und das vorhandene Wissen im Krankenhaus zusammenzutragen. Zudem sollten die Verantwortlichen für das ISMS eine Kontaktliste mit Ansprechpartnern pflegen, bei denen sie inhaltliche Fragen klären können. Darüber hinaus hat sich in verschiedenen Krankenhäusern gezeigt, dass die Wissensspeicherung und der Wissenstransfer nicht reibungslos funktionieren. Es sollten daher, falls noch nicht vorhanden, zusätzliche Prozesse zur Wissensspeicherung und -weitergabe etabliert werden.

Priorisierung besonders schützenswerter Assets

Die Etablierung eines ISMS im Krankenhaus ist ein komplexes Unterfangen. Daher ist es ratsam, die wichtigsten Sicherheitsmaßnahmen zu priorisieren und schrittweise umzusetzen. Konkret bedeutet dies, dass zunächst die besonders schützenswerten Assets im Krankenhaus identifiziert werden müssen. Anschließend sollte in enger Absprache mit der Führungsebene festgelegt werden, welche Assets in welcher Reihenfolge bearbeitet werden. Zur Unterstützung dieser Schritte können sich die Verantwortlichen am branchenspezifischen Sicherheitsstandard B3S sowie an den BSI-Standards zum ISMS orientieren. Nach der Umsetzung der wichtigsten Sicherheitsmaßnahmen für die besonders schützenswerten Assets können auf Basis der gesammelten Erfahrungen schrittweise die weiteren Assets bearbeitet werden. In der Praxis hat sich gezeigt, dass insbesondere die hauseigenen Serversysteme innerhalb der Krankenhaus-IT zu der besonders schützenswerten Kategorie gehören.

Effiziente ISMS-Etablierung

Eine kostenlose Unterstützung bieten die verschiedenen Templates und Hilfsdokumente für die Etablierung eines ISMS, die das BSI auf seiner Website zur Verfügung stellt. Diese Vorlagen enthalten Schritt-für-Schritt-Ausfüllanweisungen und bieten eine solide Grundlage für den Aufbau des theoretischen Teils eines ISMS. Zudem enthalten sie wichtige Tipps und Hilfestellungen, die den Implementierungsprozess sowie die Aufrechterhaltung des ISMS erleichtern. Somit müssen in jedem Krankenhaus keine grundlegenden Dokumente neu erstellt werden, wodurch der Fokus auf die Umsetzung der theoretischen Prozesse in die Praxis gelegt werden kann.

Um so effizient und ressourcenschonend wie möglich zu arbeiten, sollten Automatisierung und digitale Tools genutzt werden. Beispiele hierfür umfassen automatisierte Phishing-Simulationen, die in regelmäßigen Abständen an Mitarbeiter versendet werden, um deren Sensibilität gegenüber Phishing-Angriffen zu erhöhen, sowie automatisierte Schulungsprogramme, die das Personal kontinuierlich über aktuelle Bedrohungen und bewährte Sicherheitspraktiken aufklären. Bei der Umsetzung eines ISMS empfiehlt sich der Einsatz softwaregestützter Lösungen gegenüber einer manuellen Umsetzung, da diese den zeitlichen Aufwand und das Risiko einer punktuellen Umsetzung erheblich reduzieren. Eine solche Softwareunterstützung bietet aus wirtschaftlicher Perspektive klare Vorteile, insbesondere bei begrenzten verfügbaren Ressourcen. Als Orientierungshilfe stellt das BSI eine Liste zertifizierter Produkte sowie deren zugelassene Einsatzbereiche zur Verfügung.

Einbindung der Krankenhausbelegschaft

Bei der Etablierung, Weiterentwicklung und Aufrechterhaltung eines ISMS sollte die Krankenhausbelegschaft mit einbezogen werden. Dies geschieht primär durch die Schärfung des Bewusstseins der Angestellten mittels Schulungen und Informationsveranstaltungen. In der Praxis zeigte sich dabei jedoch vermehrt, dass die Mitarbeiter dies primär als lästige Pflichtveranstaltung wahrnehmen, welche sie von ihren eigentlichen Tätigkeiten im Krankenhaus abhält. Die Schulungen und Belehrungen sollten daher möglichst praxisnah und interaktiv gestaltet sein. Gab es in den vergangenen Monaten Vorfälle im Krankenhaus oder in den Medien, welche sich als Beispiele anbieten, sollten solche aufgearbeitet werden. Im realen Betrieb zeigten kurze Checklisten – als Flyer gestaltet – ebenfalls positive Auswirkungen, um Wissen zu vermitteln und auf den Ernstfall vorzubereiten. Beispiele hierfür sind Szenarien wie ein Stromausfall oder ein Ransomware-Angriff, für welche die Checklisten spezifische Handlungsempfehlungen und Maßnahmen enthalten, um in diesen kritischen Situationen schnell und effektiv reagieren zu können (Tab.). Die Erfahrung zeigt, dass im Ernstfall keine Zeit bleibt, die richtige Textpassage in einem mehrhundertseitigen Dokument zu suchen.

Zusammenfassend muss ein Krankenhaus, das ein ISMS etablieren möchte, zunächst die Führungsebene für die Umsetzung begeistern und über die Risiken von Sicherheitsmängeln aufklären. Um die verfügbaren Ressourcen effizient zu nutzen, sind zuerst die wichtigsten Assets zu identifizieren und zu schützen. Dabei ist auf bereits existierendes Wissen im Krankenhaus zurückzugreifen und die öffentlich verfügbaren Hilfsmittel des BSI einzubeziehen, da diese bewährten Methoden sowie Schritt-für-Schritt-Anleitungen zur Umsetzung bieten. Entscheidend ist, dass die sichere Wissensweitergabe innerhalb des gesamten Krankenhauses gewährleistet wird und alle Mitar-

beiter – von der Pflege bis zum Vorstand – aktiv in das ISMS einbezogen werden, da jeder Einzelne zum Schutz der Informationssicherheit beiträgt. ■

Alexander Miller
Senior Manager
KPMG AG Wirtschaftsprüfungsgesellschaft
alexandermiller@kpmg.com

Peter Maximilian Conrad
Senior Manager
KPMG AG Wirtschaftsprüfungsgesellschaft
pconrad@kpmg.com

Benjamin Rebholz
KPMG AG Wirtschaftsprüfungsgesellschaft
brebholz@kpmg.com